How to Run an On-Demand Scan with CrowdStrike

David Raco - 2023-05-01 - Comments (0) - CrowdStrike

CrowdStrike is a Next Generation AntiVirus (NGAV) that relies more on analyzing behaviors than it does on scanning files, but you can still use it to run manual scans on your computer for peace of mind. You can use the On-Demand Scan feature to scan your system drive, other drives attached to your computer, or just files on your computer that you think are suspicious or might contain malicious code.

On-Demand Scanning with CrowdStrike is only available on Windows for now.

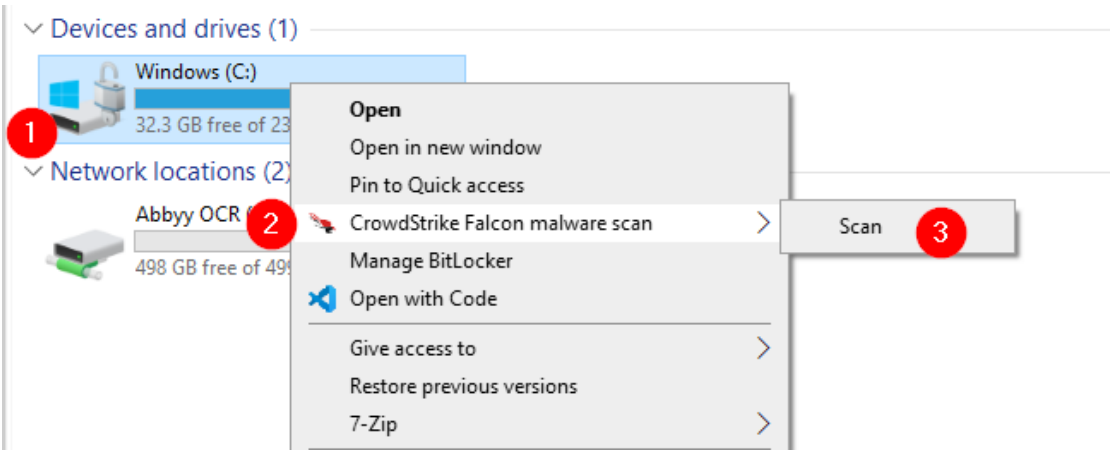
Support for On-Demand Scanning in macOS is coming. In the meantime, CrowdStrike is still protecting your Mac computer and will block malicious files from running in real time. On-demand scanning just enables you to scan a file before executing it. It's not necessary to do that with Next Generation AntiVirus, but CrowdStrike supports it as a peace of mind feature on Windows and will support it soon for macOS.

When running an On-Demand Scan, CrowdStrike will only alert you if it detects something! It is normal to not get any feedback if the scan turns up clean!

Scanning Drives in Windows

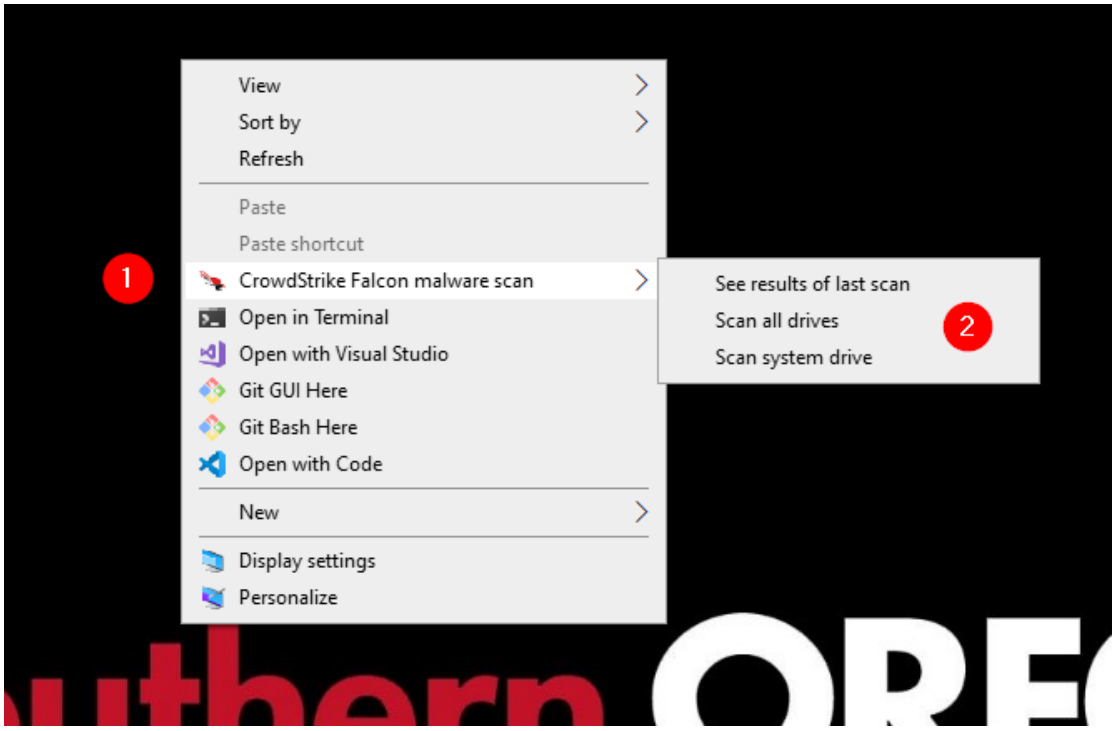
Be aware that scanning a large drive full of files could take a long time! CrowdStrike is very efficient with its scans, only looking at files that could potentially execute code, but you should still be prepared to give it some time.

You can scan any drive attached to your computer by right-clicking it in File Explorer and selecting the Scan option from the CrowdStrike Falcon menu.



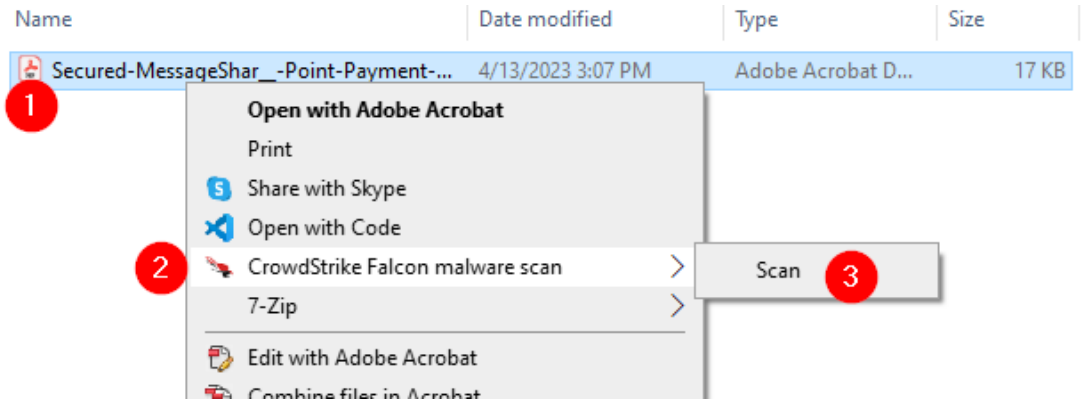
You can also find convenient drive scan options in the CrowdStrike menu from right-clicking on your Desktop. You can scan all drives, scan just your system drive (usually C: on Windows), or see the results of your last scan. Using the "see results of last scan" option is usually unnecessary since CrowdStrike will alert you to anything it finds when you run a scan. No news is good news, but you're welcome to use the "see results of last scan" option

if you want confirmation that the scan completed.



Scanning Files and Folders in Windows

You can easily scan individual files or folders by selecting a single file or folder in File Explorer or on your Desktop, then right-clicking it to bring up the right-click menu. From there, select CrowdStrike Falcon and then click Scan.



Currently this doesn't work for multiple files or folders selected at the same time! If you need to scan multiple files or folders, either put them all into one folder and scan that folder, or scan the entire parent folder that contains all the files and folders you want to scan.

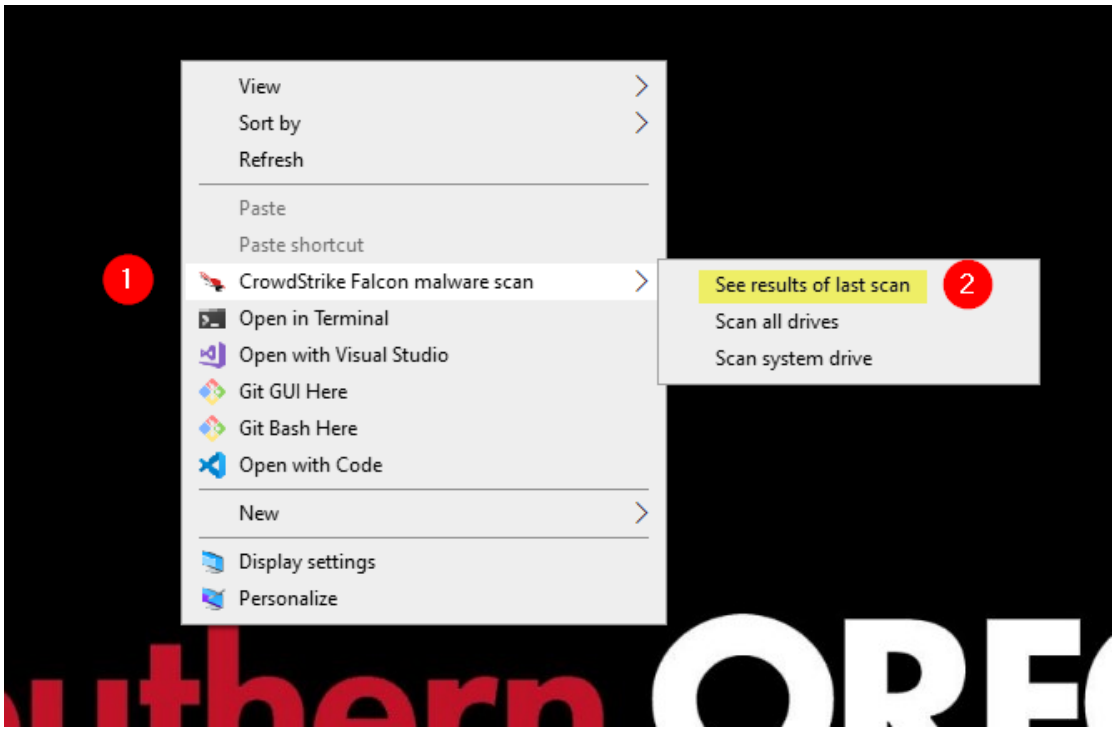
What to Do If CrowdStrike Detects Malware

If CrowdStrike detects something malicious on your computer, don't panic. It's good that you caught it "at rest" before it could execute and potentially harm your computer. CrowdStrike will automatically report any detections to the Information Security Manager for review, but we also encourage you to email infosec@sou.edu with additional details you can provide for context. For example, if CrowdStrike detects a malicious executable

in your Downloads folder, do you remember where you downloaded it from and when?

What to Do If CrowdStrike Doesn't Show Anything

No news is good news when it comes to On-Demand Scanning with CrowdStrike. Ideally, you run the scan and nothing happens. If you want to confirm that the scan actually executed, you're welcome to use the "see results of last scan" option which you can access from your Desktop. Just right-click anywhere on your Desktop, go to the CrowdStrike Falcon menu, and then click on the "See results of last scan" submenu option.



You should then see a black terminal window pop up on your screen with details of the scan. It's normal to see many "unsupported files" in the tally because CrowdStrike doesn't waste time scanning files that are incapable of running code on your computer, such as image files. You should see zero suspicious files in the tally, otherwise CrowdStrike would have alerted you.

